OXFORD COMPUTER GROUP

TD SYNNEX

IDABUS®

Riskante mobile Endgeräte und deren Einfluss

Solution Architect

Andreas Zemla

OCG

OXFORD COMPUTER GROUP

01

Eine Person. Viele Konten.
Eine Sicherheitsentscheidung.

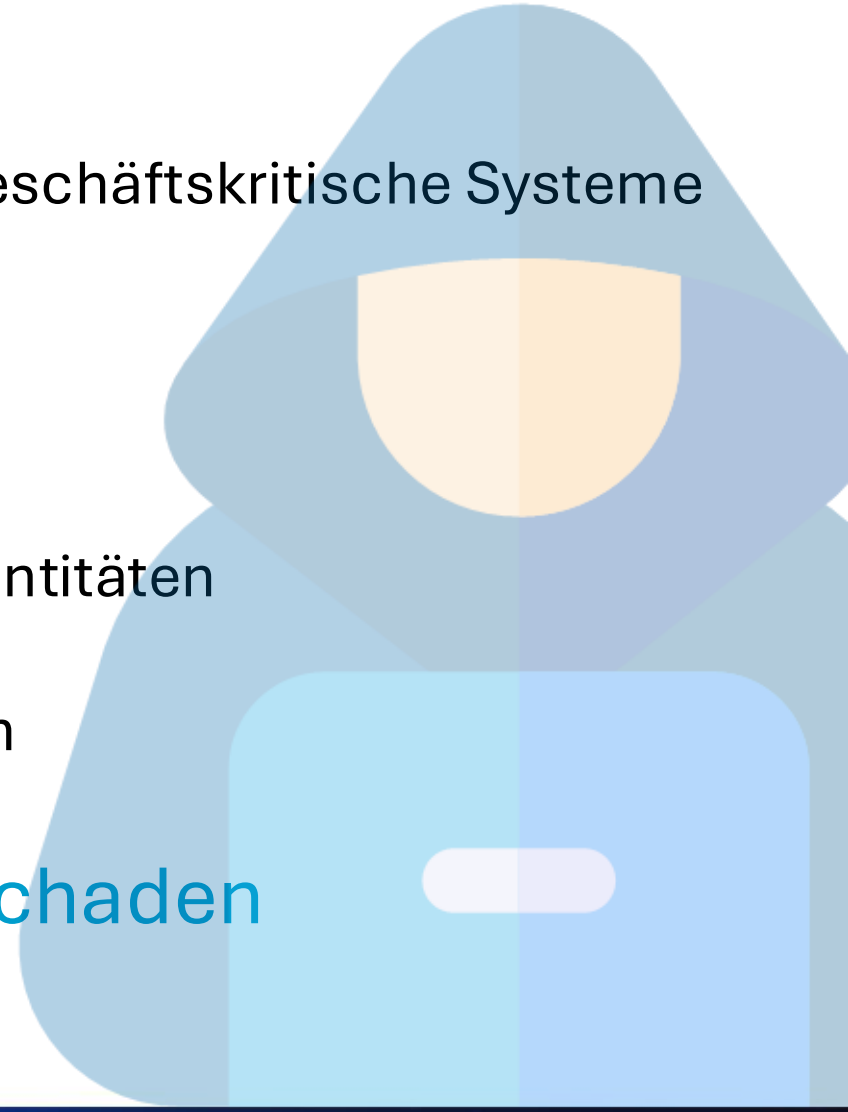
Eine Person. Viele Konten.

- Eine Person, gerade im administrativen Bereich, kann mehrere Benutzerkonten besitzen:
  - Standard Account
  - AI-Agenten
  - AD Admin
  - Azure Admin
  - M365 Admin
  - SAP Admin
  - DB Admin
  - ….
- Eine Person kann mehrere kritische Geschäftsrollen und/oder mehrere PAM-Kandidaturen innehaben:
  - Global Admin
  - Domain Admin
  - Enterprise Admin
  - SAP-Zeichnungsberechtigung
  - ….

Der Angreifer sucht kein System, sondern eine Identität.

Die Realität moderner Angriffe

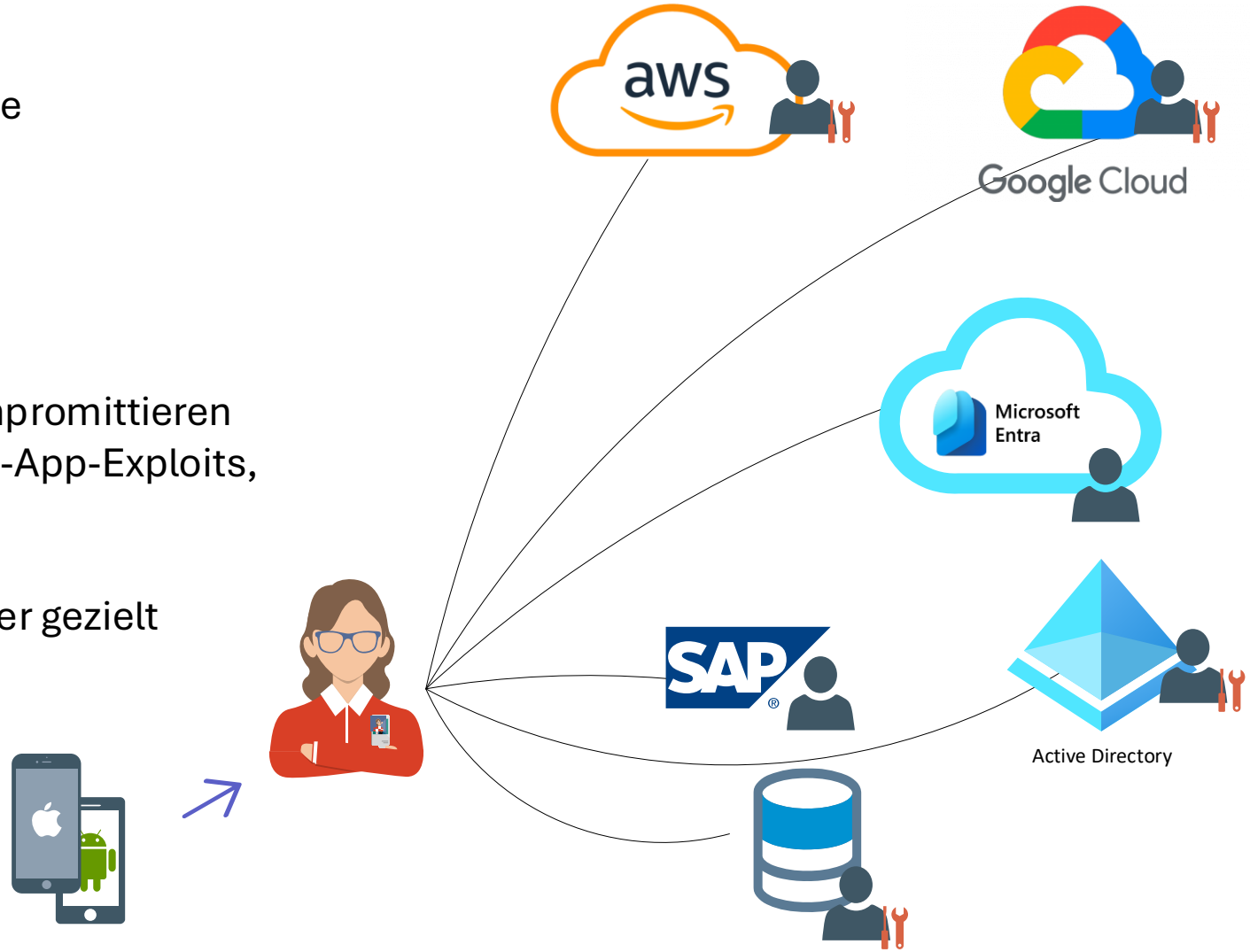
Benutzer → Smartphone → Cloud → Privileged Access → Geschäftskritische Systeme



- Angriffe beginnen sehr häufig am Endgerät
- Kompromittierte Geräte führen zu kompromittierten Identitäten
- Gestohlene Identitäten führen zu privilegierten Zugriffen
- Die Reaktionszeit entscheidet über den Schaden

Die Realität moderner Angriffe

- 30 % aller Cyberangriffe nutzen gestohlene Konten als Einstiegspunkt (Quelle: IBM)
- Die Vielzahl an normalen Benutzerkonten vergrößert die Angriffsfläche erheblich
- Low-Privilege-Konten sind leichter zu kompromittieren (Credential Theft, Session Hijacking, Web-App-Exploits, Phishing, Passwortreuse, MFA-Bypass…)
- Sobald ein Angreifer im System ist, sucht er gezielt nach Wegen zur Rechteausweitung.
  (78 % aller erfolgreichen Breaches enthalten Privilege Escalation)

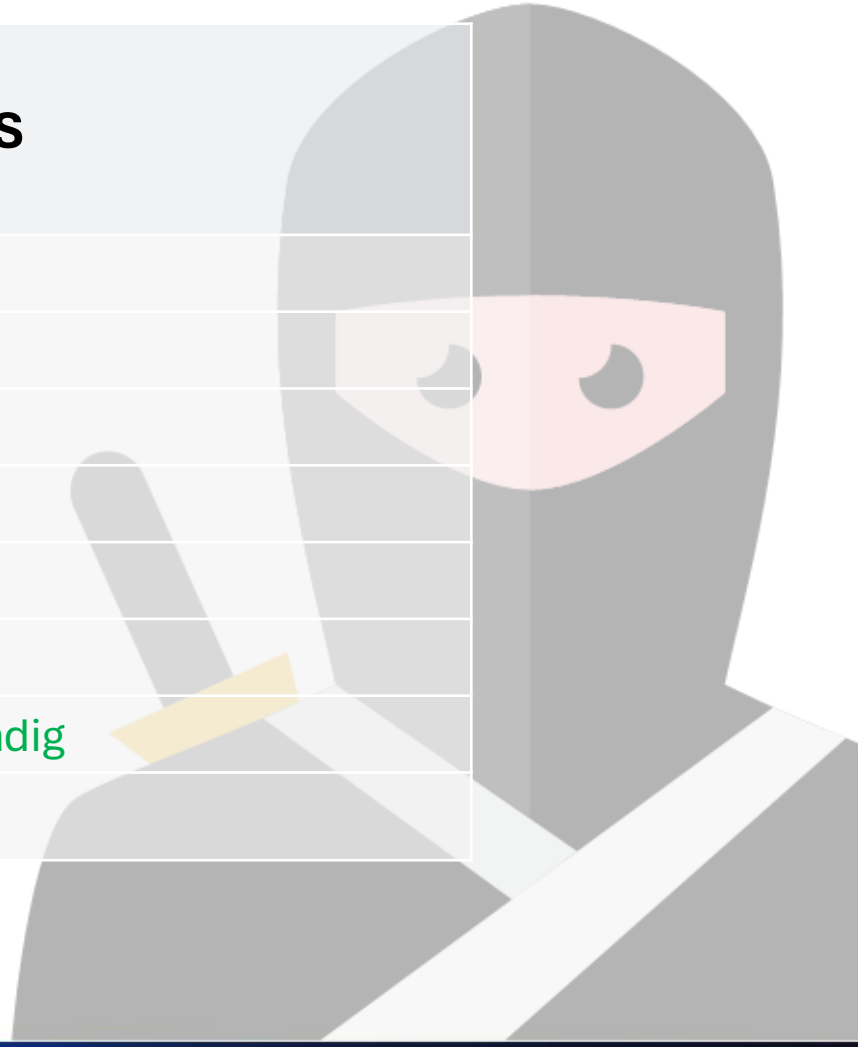


Warum klassischen IAM-Lösungen nicht ausreichen?

Klassisches IAM	IDABUS
▪ Identitäten verwalten	▪ Identitäten verwalten und schützen
▪ Provisionierung	▪ Automatisierte Verteidigung
▪ Statische Rollen	▪ Dynamisches Risiko
▪ Governance	▪ Governance + Security
▪ Reaktive Prozesse	▪ Echtzeit-Reaktion (Proaktiv)
▪ Identitäten ohne gelinkten Accounts	▪ Ganzheitliche Betrachtung einer Identität
▪ Berücksichtigt keine externen Trigger	▪ Integrierte Risk-Engine

Was macht IDABUS einzigartig?

Funktion	Klassisches IAM	IDABUS
Provisionierung	✓	✓
RBAC	✓	✓
Governance	✓	✓
Echtzeit-Risiko	✗	✓
Security Automation	✗	✓
Threat Response	✗	✓
Identity Security	Teilweise	Vollständig
Risk Driven Access	✗	✓



Risk-Engine Architektur

Log Stream
Push/Pull
Webservice

Nachrichtenauswertung
und Filterung

Monitoring,
Reporting
und Automatisierung

OXFORD COMPUTER GROUP

02

Live Demo

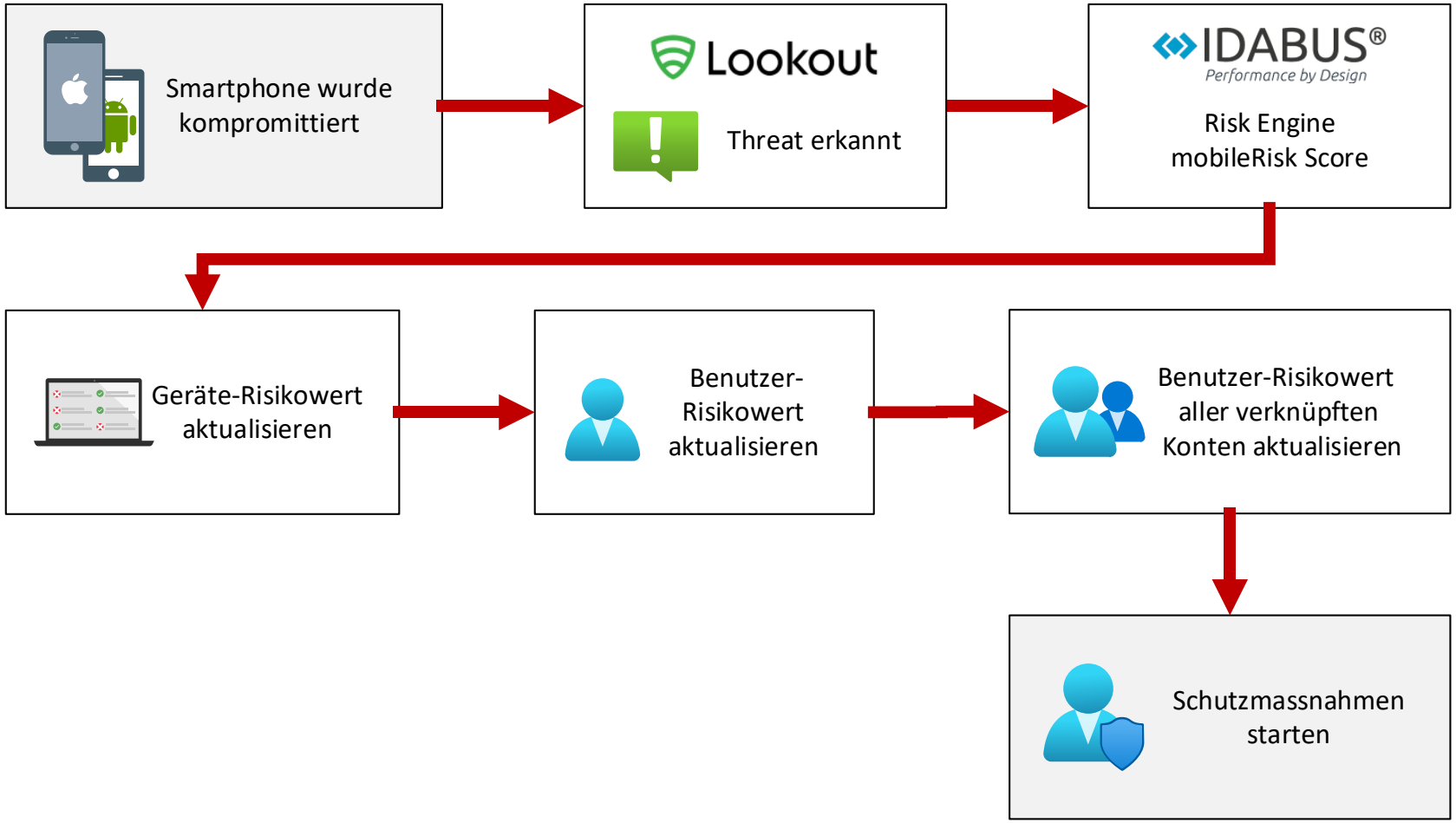
Lass uns ein Gerät kompromittieren.

OXFORD COMPUTER GROUP

Die Ausgangssituation

Aktive Reaktion auf Bedrohungen

Prozessdiagramm



Mögliche Schutzmaßnahmen

- Teilweise-Entrechtung
  - Entzug von kritischen Gruppenmitgliedschaften
  - Entzug von kritischen Rollen

- PIM/PAM-Prozesse
  - PAM-Kandidaturen filtern
  - Aktive Sitzungen schließen

- Administratorkonten teilweise sperren
- Vollständige Kontensperrung
- Service Desk informieren
- Security Team informieren
- Audit Event erstellen

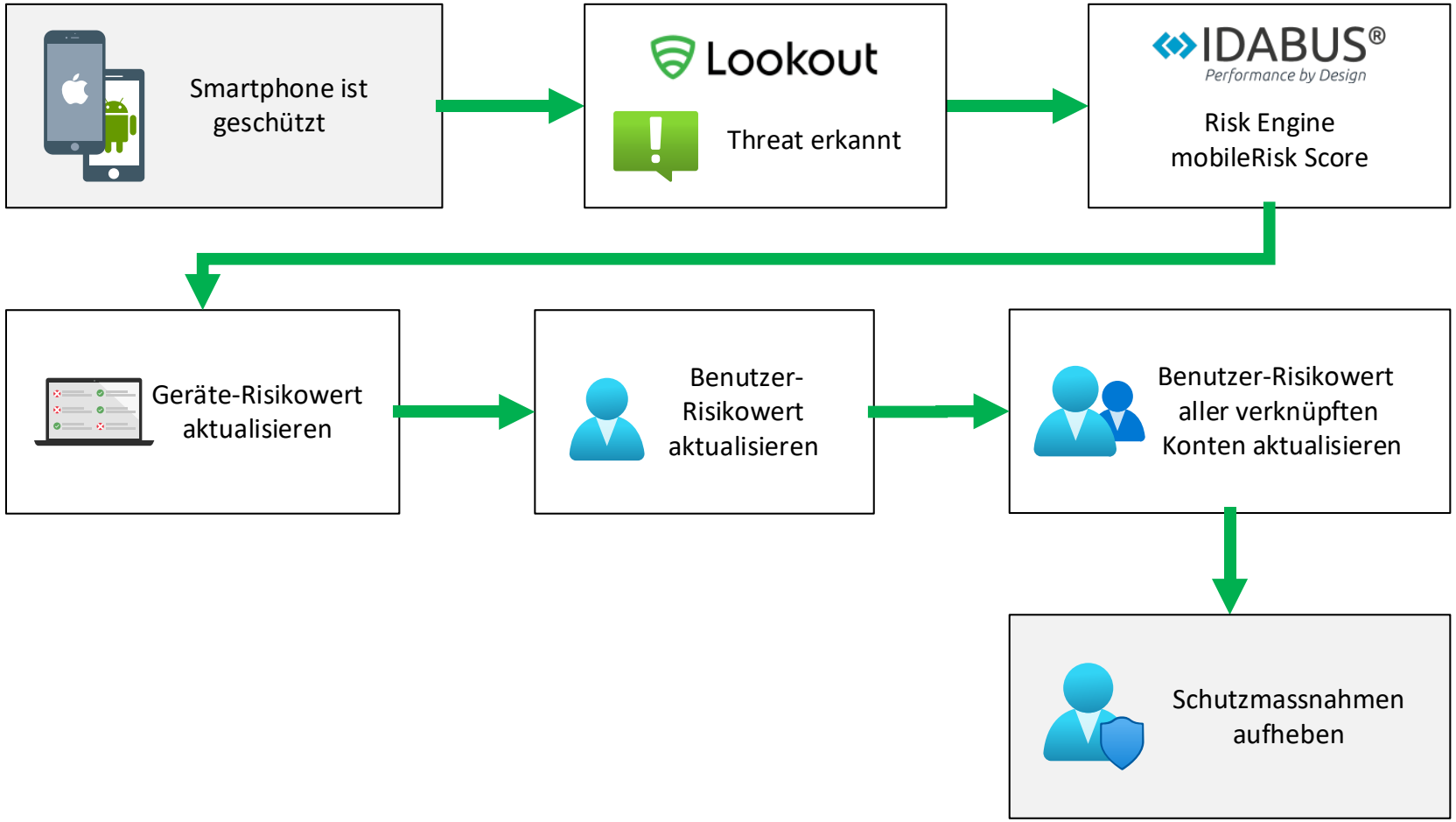
Live Demo

OXFORD COMPUTER GROUP

Smartphone wird kompromittiert

Wiederherstellung

Prozessdiagramm



Live Demo

OXFORD COMPUTER GROUP

Rechte-Wiederherstellung

03

Zusammenfassung

Was macht IDABUS einzigartig?

- Klassische IAM-Systeme verwalten Identitäten.
  IDABUS nutzt Identitäten aktiv zur Abwehr von Cyberbedrohungen.

- IDABUS kennt die Beziehungen zwischen Benutzern, Geräten, Standardkonten, Privileged Accounts, Benutzergruppen und Rollen und kann gezielt und automatisch auf identitätsbasierte Risiken reagieren.

- Die Identität wird zum Durchsetzungspunkt für Mobile Threat Intelligence

- Die IDABUS-Plattform ist eine Lösung für Identity Management, Identity Governance und Identity-driven Security in hybriden Umgebungen.

Eine Identität - Hybrider Schutz

- Ein kompromittiertes Smartphone gefährdet nicht nur ein Benutzerkonto.
- Es gefährdet alle Identitäten, die mit dieser Person verbunden sind.
- IDABUS kennt diese Beziehungen und schützt Cloud- und On-Premises-Umgebungen gleichzeitig.

Business Value

Reduzierung	Erhöhung
▪ Reaktionszeit	▪ Sicherheit
▪ Angriffsfläche	▪ Compliance
▪ Privileged Exposure	▪ Transparenz
▪ Manuelle Tätigkeiten	▪ Automatisierung


OXFORD
COMPUTER GROUP
IDABUS®
TD SYNNEX